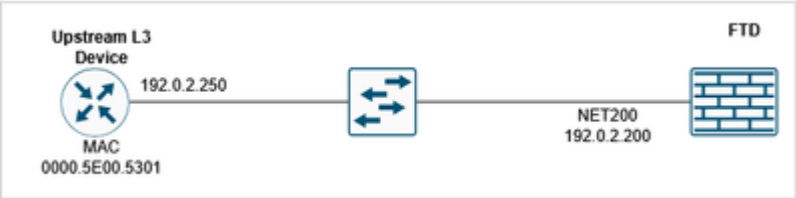
Dépannage de FTD Impossible d'envoyer une requête ping au périphérique en amont malgré l'entrée ARP

Table des matières

Problème

La défense contre les menaces de pare-feu (FTD) n'a pas pu envoyer de requête ping à l'adresse IP du périphérique en amont, bien que le pare-feu ait pu observer l'entrée ARP pour l'adresse IP en amont. La table ARP affichait les entrées attendues, indiquant que la connectivité de couche 2 fonctionnait mais que le trafic ping de couche 3 était bloqué.

Topologie



Symptômes CLI FTD

Échec de la commande ping vers l'adresse IP en amont :

<#root>

```
device#
```

ping 192.0.2.250

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.0.2.250, timeout is 2 seconds:
?????
Success rate is 0 percent (0/5)
```

Il existe une entrée ARP pour l'adresse IP en amont :

<#root>

```
device#
```

show arp

NET200 192.0.2.250 0000.5e00.5301

47

Activez une capture avec trace sur l'interface FTD :

<#root>

```
device#
```

capture CAPI interface NET200 trace match icmp host 192.0.2.200 host 192.0.2.250

FTD LINA syslogs pendant le test ping :

<#root>

```
device#
```

show log | include 192.0.2.250

```
May 15 2026 09:46:26: %FTD-6-302020: Built outbound ICMP connection for faddr 192.0.2.250/0 gaddr 192.0
May 15 2026 09:46:26: %FTD-3-313001:
```

Denied ICMP type=0, code=0 from 192.0.2.250 on interface NET200

```
May 15 2026 09:46:26: %FTD-6-302021: Teardown ICMP connection for faddr 192.0.2.250/0 gaddr 192.0.2.200
...
```

La capture de paquets montre les réponses d'écho ICMP arrivant :

```
<#root>

device#

show capture CAPI



10 packets captured
   1: 09:46:26.649456       802.1Q vlan#200 P0 192.0.2.200 > 192.0.2.250 icmp: echo request
   2: 09:46:26.649883       802.1Q vlan#200 P0 192.0.2.250 > 192.0.2.200 icmp:

echo reply



   3: 09:46:28.642621       802.1Q vlan#200 P0 192.0.2.200 > 192.0.2.250 icmp: echo request
   4: 09:46:28.643002       802.1Q vlan#200 P0 192.0.2.250 > 192.0.2.200 icmp:

echo reply



...
```

La trace de paquet de la réponse d'écho ICMP indique que le paquet correspond à une connexion existante comme prévu et que l'interface de sortie est l'interface FTD (NP Identity Ifc) :

```
<#root>

device#

show capture CAPI packet-number 2 trace



10 packets captured
   2: 09:46:26.649883       802.1Q vlan#200 P0 192.0.2.250 > 192.0.2.200 icmp:

echo reply



...
Phase: 3
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Elapsed time: 4096 ns
Config:
Additional Information:
```

Found flow with id 1400, using existing flow

...

Result:
input-interface: NET200(vrfid:0)
input-status: up
input-line-status: up

output-interface: NP Identity Ifc

Action: allow
Time Taken: 28672 ns

Debug ICMP trace indique que la réponse d'écho ICMP est refusée :

<#root>

FTD220-5#

debug icmp trace

debug icmp trace enabled at level 1

FTD220-5#

ping 192.0.2.250

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.0.2.250, timeout is 2 seconds:
ICMP echo request from self:192.0.2.200 to NET200:192.0.2.250 ID=49503 seq=15001 len=72

ICMP echo reply

from NET200:192.0.2.250 to self:192.0.2.200

ID=49503 seq=15001 len=72

Denied ICMP type = 0, code = 0 from 192.0.2.250on interface 4

?
...
Success rate is 0 percent (0/5)

⚠Mise en garde : Utilisez les débogages avec prudence !

Pour désactiver le débogage ICMP :

<#root>

```
device#

no debug icmp trace


debug icmp trace disabled.
```

Environnement

FTD 10.x. D'autres versions logicielles sont également affectées.

Résolution

Le problème a été résolu en identifiant et en corrigeant une configuration de règle ICMP dans les paramètres de la plate-forme refusant le trafic ping.

La résolution comportait les étapes suivantes :

Étape 1 : vérification des entrées de la table ARP

Vérifiez que les entrées ARP pour l'adresse IP en amont sont visibles dans la table ARP du pare-feu, ce qui indique que la connectivité de couche 2 fonctionne correctement :

<#root>

```
device#

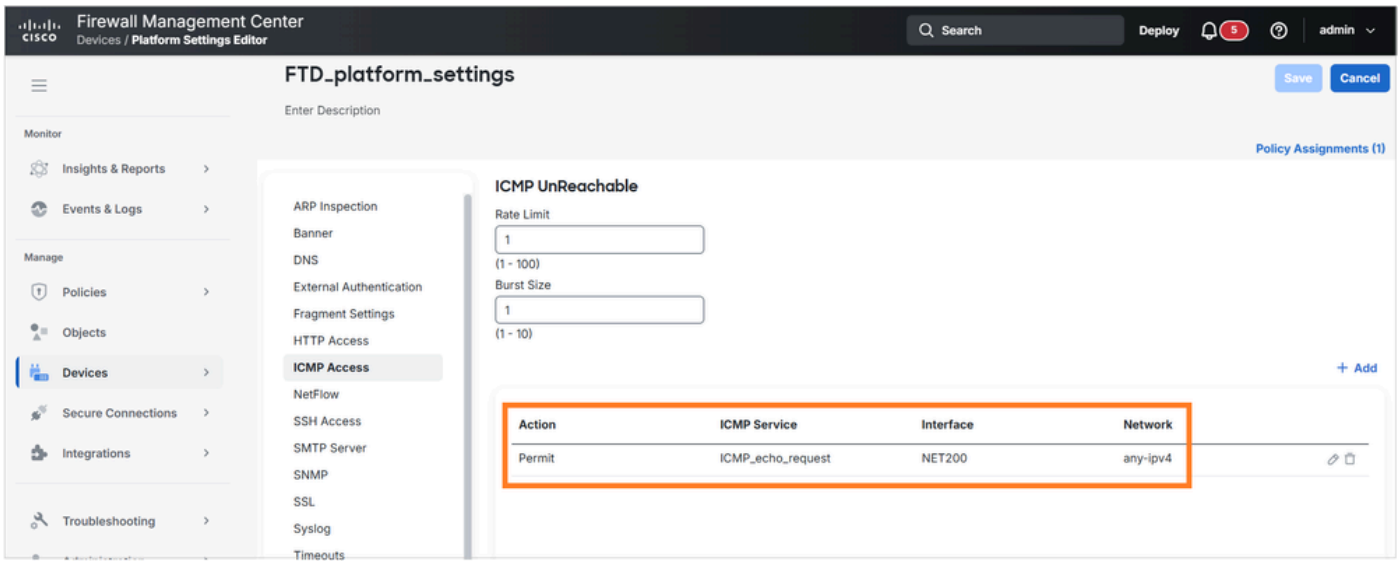
show arp
```

Étape 2 : vérification des règles ICMP dans les paramètres de la plate-forme

Accédez à la configuration des paramètres de la plate-forme et examinez les politiques de règles ICMP qui peuvent affecter le trafic ping. Recherchez spécifiquement les règles qui pourraient bloquer ou refuser les paquets de requête/réponse d'écho ICMP.

Étape 3 : identification et modification de la règle ICMP de blocage

Localisez la règle ICMP dans les paramètres de la plate-forme qui est configurée pour refuser le trafic ping.



Dans cet exemple, la règle ICMP autorise uniquement les requêtes d'écho ICMP à être acceptées par l'interface FTD.

Vérification CLI FTD :

```
<#root>
```

```
device#

show run icmp


icmp unreachable rate-limit 1 burst-size 1

icmp permit any echo NET200
```

Étape 4. Mise à jour de la configuration des règles ICMP

Modifiez la règle ICMP identifiée pour autoriser le trafic ping ou supprimez la configuration de blocage en fonction des exigences de sécurité du réseau et des besoins opérationnels.



La règle ICMP résultante :

<#root>

```
device#

show run icmp


icmp unreachable rate-limit 1 burst-size 1
icmp permit any echo NET200

icmp permit 192.0.2.0 255.255.255.0 echo-reply NET200
```

Étape 5. Test de la connectivité

Après avoir effectué les modifications de configuration, testez la connectivité ping à l'adresse IP en amont pour vérifier que le problème a été résolu et que le trafic ICMP circule désormais correctement :

<#root>

```
device#

ping 192.0.2.250


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.0.2.250, timeout is 2 seconds:
!!!!!

Success rate is 100 percent (5/5)

, round-trip min/avg/max = 1/1/1 ms
```

Motif

La cause principale de ce problème était une règle ICMP configurée dans les paramètres de la plate-forme qui refusait explicitement le trafic des réponses d'écho ICMP. Alors que le pare-feu maintenait une connectivité de couche 2 correcte (mise en évidence par les entrées ARP visibles), la règle ICMP au niveau de la plate-forme bloquait les paquets de réponse d'écho ICMP de couche 3, empêchant ainsi les opérations ping réussies vers l'adresse IP en amont. Ce type de configuration peut se produire lorsque des stratégies de sécurité sont mises en oeuvre pour limiter le trafic ICMP, mais peut affecter par inadvertance le test et la surveillance de la connectivité réseau légitime.

Autres informations utiles

- Configurer l'accès ICMP
- icmp
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.